



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/638,661	08/14/2000	Nimrod Megiddo	ARC9-2000-0077-US1	9660

33360 7590 04/07/2004

MARK D. MCSWAIN  
IBM ALMADEN RESEARCH CENTER, IP LAW DEPT.  
650 HARRY ROAD  
CHTA/J2B  
SAN JOSE, CA 95120

EXAMINER

NORRIS, TREMAYNE M

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 04/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/638,661

Applicant(s)

MEGIDDO ET AL.

Examiner

Tremayne M. Norris

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 14 August 2000.  
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-5, 7-25 and 27-33 is/are rejected.  
7) ☒ Claim(s) 6, 26, 34-36 is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☒ The drawing(s) filed on 14 August 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 2.  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_.

**DETAILED ACTION**

***Claim Rejections - 35 USC § 112***

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 11-13 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. In claim 11, the steps found in lines 3-6 are not taught in the specification.

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 10-13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 10 recites the limitation "the secure suffixes" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Art Unit: 2137

5. Claims 15-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 15 recites the limitation "said encryption keys" in line 1. There is insufficient antecedent basis for this limitation in the claim. Regarding claim 16, it is unclear as to where or when the "decrypted encryption key" is first encrypted.

6. Claim 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 20 recites the limitation "new secure suffix" in line 4. There is insufficient antecedent basis for this limitation in the claim.

7. Claims 21-23 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 21 recites the limitation "the secure suffix" in line 1 of claim 21 on page 17. There is insufficient antecedent basis for this limitation in the claim.

8. Claims 30-32 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 30 recites the limitation "the

Art Unit: 2137

secure suffix" in line 2. There is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 102***

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-4,14,15,24,25,32 are rejected under 35 U.S.C. 102(e) as being anticipated by Sasaki (US pat 6,351,536).

Regarding claim 1, Sasaki teaches a method of selectively making information available to groups of parties amongst a plurality of parties, said method comprising the steps of

- a) generating a public key (col.1 lines 55-61);
- b) publishing said public key (col.1 lines 27-30);
- c) generating a secure key (col.1 lines 55-61);
- d) combining said secure key with said public key (col.1 lines 19-22); and,
- e) distributing a key corresponding to said secure key to members of a selected group (col.2 lines 4-7; col.2 lines 20-22; col.5 lines 36-39).

Regarding claim 2, Sasaki teaches a method as in claim 1, wherein the public key is a recognizable name portion and the step (a) of generating a public key comprises generating a plurality of public keys (col.2 lines 14-19).

Regarding claim 3, Sasaki teaches a method of claim 2, wherein in step (d) said secure key is combined with each of said plurality of public keys (col.1 lines 19-22; col.2 lines 17-19).

Regarding claim 4, Sasaki teaches a method of claim 3, wherein in step (d) said secure key is combined with ones of said plurality of public keys (col.1 lines 19-22; col.2 lines 17-19).

Regarding claim 14, Sasaki teaches a method as in claim 1, wherein the secure keys are encrypted keys and the corresponding keys are decryption keys (col.1 line 66 thru col.2 line 3; col.2 lines 36-46).

Regarding claim 15 (as best understood), Sasaki teaches a method as in claim 14, wherein said encryption keys are combined with one or more links, said links combined with encrypted keys being published as encrypted links (col.23 lines 33-37; col.24 lines 29-37).

Art Unit: 2137

Claims 24,25,32 are substantially equivalent to claims 1,4,12 respectively, therefore claims 24,25,32 are rejected because of similar rationale.

***Claim Rejections - 35 USC § 103***

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims 5,10,12,31 rejected under 35 U.S.C. 103(a) as being unpatentable over Sasaki, and further in view of Vobach (US pat 5,193,115).

Regarding claim 5, Sasaki teaches a method as in claim 2 of generating a secure key, but does not teach generating a plurality of random suffixes. Vobach teaches generating a plurality of random suffixes (col.7 lines 16-23). It would have been obvious to one of ordinary skill in the art to combine Sasaki's encryption network system with Vobach's teaching of using random suffixes in order to confuse hackers/attackers (Vobach line 16).

Regarding claim 10, Sasaki and Vobach teach a method as in claim 5, in addition Sasaki teaches the secure suffixes are encrypted keys and the corresponding keys are decryption keys (col.1 line 66 thru col.2 line 3).

Regarding claim 12 (as best understood), Sasaki and Vobach teach a method as in claim 10, in addition Sasaki teaches distributing the decryption keys to group members comprising sending e-mail to members of the selected group (col.3 lines 40-48).

Claim 31 is substantially equivalent to claim 12, therefore claim 31 is rejected because of similar rationale.

13. Claims 7-9,19,27-29,33 rejected under 35 U.S.C. 103(a) as being unpatentable over Sasaki and Vobach, and further in view of Win et al (US pat 6,453,353).

Regarding claim 7, Sasaki and Vobach teach a method as in claim 5 of distributing random suffixes to members, but do not teach members of one or more selected groups, at least one selected group not receiving one or more distributed keys. Win et al teach providing access to resources to members of one or more selected groups, and denying access to at least one selected group (col.2 lines 40-56; col.3 lines 1-6; col.5 lines 33-65). It would have been obvious to one of ordinary skill in the art to combine Sasaki and Vobach's encryption network system of distributing keys to access encrypted information with Win et al's role-based distribution of resources in order to provide an enciphering



Art Unit: 2137

method in which encryption communication can be established safely and simply through a network utilized by a plurality of grouped transmitters and receivers (Sasaki col.1 lines 36-41).

Regarding claim 8, Sasaki, Vobach, and Win et al teach a method as in claim 7, in addition Sasaki teaches group members use received said random suffixes to access secure information (col.1 line 65 thru col.2 line 3).

Regarding claim 9, Sasaki, Vobach, and Win et al teach a method as in claim 8, in addition Win et al teach the secure information is contained on a web page, each web page containing secure information being identified by one of said random suffixes (col.2 lines 54-56).

Regarding claim 19, Sasaki and Vobach teach a method as in claim 5, but do not teach changing secure page names for a selected group. Win et al teach changing a secure page name for a selected group (col.13 lines 8-16; col.14 lines 33-55).

Claim 27-29, and 33 are substantially equivalent to claims 7-9, and 19, therefore claims 27-29 and 33 are rejected because of similar rationale.

Art Unit: 2137

14. Claims 16-18 (as best understood) rejected under 35 U.S.C. 103(a) as being unpatentable over Sasaki, and further in view of Chang et al.

Regarding claim 16, Sasaki teaches a method of claim 15, but does not teach a client browser automatically prompts a user for a decryption key whenever an encrypted link is encountered, said browser decrypting the encrypted link using the decryption key and, responsive to the decrypted encryption key requesting a corresponding web page. Chang et al do teach a client browser automatically prompts a user for a decryption key whenever an encrypted link is encountered, said browser decrypting the encrypted link using the decryption key and, responsive to the decrypted encryption key requesting a corresponding web page (col.11 lines 34-48; col.12 lines 37-49). It would have been obvious to one of ordinary skill in the art to combine Sasaki's encryption network system with Chang et al's teaching of a browser decrypting encrypted links in order to have the browser read the content received in encrypted form and perform the appropriate procedures to enable the user to read a HTML document (Chang col.11 lines 30-33).

Regarding claim 17, Sasaki and Chang et al teach a method as in claim 16, in addition Chang et al teach the file corresponding to an encrypted link is encrypted (col.11 lines 34-48).

Art Unit: 2137

Regarding claim 18, Sasaki and Chang et al teach a method as in claim 16, in addition Chang et al teach said client browser automatically decrypts the corresponding encrypted file using a locally stored private decryption key (col.11 lines 34-48).

***Allowable Subject Matter***

15. Claims 6,26,34-36 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The following is a statement of reasons for the indication of allowable subject matter:

With respect to claim 6, the cited prior art fails to specifically teach a method as in claim 5, wherein in the combining step (d), said random suffixes are concatenated with ones of said plurality of public keys.

With respect to claim 26, the cited prior art fails to specifically teach a computer program product as in claim 24, wherein the secure keys are random suffixes and the combining means concatenates said random suffixes with ones of said plurality of public keys.

With respect to claim 34, the cited prior art fails to specifically teach a computer program product as in claim 33, wherein the computer readable program code means for changing secure page names comprises:

computer readable program code means for removing a secure key from said secure page name;

computer readable program code means for attaching a new secure key;  
and

computer readable program code means for sending e-mail to members of said selected group, informing said members of said secure name change.

With respect to claim 35, the cited prior art fails to specifically teach a computer program product as in claim 24, wherein the computer readable program code means for generating random suffixes comprises:

computer readable program code means for generating a plurality of random numbers between 0 and 61; and

computer readable program code means for mapping each of said plurality of random numbers to a corresponding alphanumeric number.

With respect to claim 36, the cited prior art fails to specifically teach a computer program product as in claim 35, wherein the mapped plurality of random numbers generated is a decryption key. the computer readable program code means for generating random suffixes further comprising:

Art Unit: 2137

computer readable program code means for deriving an encryption key from said generated decryption key.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (703) 305-8045. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 305-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

April 2, 2004

*Matthew Smithers*  
MATTHEW SMITHERS  
PRIMARY EXAMINER  
*Art Unit 2137*